



Japan Patent Office

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: January 20, 2004

Application Number: Japanese Patent Application
No.2004-012239

[ST.10/C]: [JP2004-012239]

Applicant(s): RICOH COMPANY, LTD.

February 6, 2004

Commissioner,
Japan Patent Office

Yasuo Imai (Seal)

Certificate No.2004-3007636

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2004年 1月20日

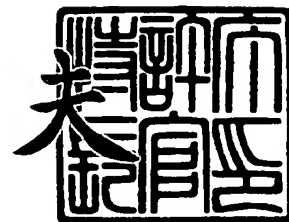
出願番号
Application Number: 特願2004-012239
[ST. 10/C]: [JP2004-012239]

出願人
Applicant(s): 株式会社リコー

2004年 2月 6日

特許庁長官
Commissioner,
Japan Patent Office

今井 康



出証番号 出証特2004-3007636

【書類名】 特許願
【整理番号】 0308943
【提出日】 平成16年 1月20日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 H04N 1/41
【発明者】
 【住所又は居所】 鳥取県鳥取市千代水1丁目100番地 アイシン千代水ビル リ
 コー鳥取技術開発株式会社内
 【氏名】 西村 隆之
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 野水 泰之
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 作山 宏幸
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 原 潤一
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 松浦 熱河
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 矢野 隆則
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 児玉 卓
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 宮澤 利夫
【発明者】
 【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内
 【氏名】 新海 康行
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2003- 13591
 【出願日】 平成15年 1月22日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1

●)
【物件名】 要約書 1
【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

画素値を順次ランダム化することにより画像をスクランブルする画像符号化装置であって、

先にランダム化した画素値のずらし量に基づき、暗号化関数を用いて、ランダム化する画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする画像符号化装置。

【請求項 2】

請求項 1 記載の画像符号化装置であって、

前記スクランブル化手段は、前記暗号化関数の値の有効桁数に基づき、前記ランダム化する画素値のずらし量を調整することを特徴とする画像符号化装置。

【請求項 3】

請求項 1 記載の画像符号化装置であって、

前記スクランブル化手段は、程度因子に基づき、前記ランダム化する画素値のずらし量を調整することを特徴とする画像符号化装置。

【請求項 4】

請求項 1 乃至 3 いずれが一項記載の画像符号化装置であって、

前記スクランブル化手段は、前記先にランダム化した画素値のずらし量とパスワードとに基づき、前記ランダム化する画素値のずらし量を算出することを特徴とする画像符号化装置。

【請求項 5】

請求項 1 乃至 4 いずれか一項記載の画像符号化装置であって、

前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段をさらに備え、

前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とする画像符号化装置。

【請求項 6】

請求項 5 記載の画像符号化装置であって、

前記圧縮符号化手段は、J P E G 2 0 0 0 に基づき前記画像を圧縮符号化することを特徴とする画像符号化装置。

【請求項 7】

請求項 5 または 6 記載の画像符号化装置であって、

前記画像のスクランブル化及び圧縮符号化に係る情報を電子透かしとして前記符号列に埋め込む電子透かし埋め込み手段をさらに備えることを特徴とする画像符号化装置。

【請求項 8】

請求項 1 乃至 7 いずれか一項記載の画像符号化装置であって、

前記スクランブル化手段は、前記ランダム化する画素値の直前にランダム化した画素値のずらし量に基づき、前記ランダム化する画素値のずらし量を算出することを特徴とする画像符号化装置。

【請求項 9】

請求項 6 乃至 8 いずれか一項記載の画像符号化装置であって、

前記圧縮符号化手段は、J P E G 2 0 0 0 の非可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、係数量子化手段の後に設けられ、量子化された離散ウェーブレット変換係数をランダム化することを特徴とする画像符号化装置。

【請求項 10】

請求項 6 乃至 8 いずれか一項記載の画像符号化装置であって、

前記圧縮符号化手段は、J P E G 2 0 0 0 の可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、離散ウェーブレット変換手段の前に設けられ、画素値をランダム化することを特徴とする画像符号化装置。

【請求項 11】

請求項 9 記載の画像符号化装置であって、

前記スクランブル化手段は、量子化としてビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化することを特徴とする画像符号化装置。

【請求項 12】

請求項 11 記載の画像符号化装置であって、

前記スクランブル化手段は、スクランブル化されるビット係数を反転させる場合には隣桁のビット係数を反転させることを特徴とする画像符号化装置。

【請求項 13】

請求項 11 又は 12 記載の画像符号化装置であって、

前記スクランブル化手段は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。

【請求項 14】

請求項 13 記載の画像符号化装置であって、

前記スクランブル化手段は、ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。

【請求項 15】

請求項 13 記載の画像符号化装置であって、

離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。

【請求項 16】

請求項 13 記載の画像符号化装置であって、

離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。

【請求項 17】

請求項 1 乃至 16 のいずれか一項記載の画像符号化装置によりスクランブルされた符号データを画像に復号化する、複数の手段よりなる復号化手段と、

前記復号化手段を構成する前記複数の手段の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、を備えることを特徴とする符号復号化装置。

【請求項 18】

画素値を順次ランダム化することにより画像をスクランブルする方法であって、

先にランダム化した画素値のずらし量に基づき、暗号化関数を用いて、ランダム化する画素値のずらし量を算出するスクランブル化過程を有することを特徴とする画像符号化方法。

【請求項 19】

請求項 18 記載の画像符号化方法によりスクランブルされた符号データを画像に復号化する、複数の過程よりなる復号化過程と、

前記復号化過程を構成する前記複数の過程の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化過程と、を備えることを特徴とする符号復号化方法。

【請求項 20】

コンピュータに、画素値を順次ランダム化することにより画像をスクランブルさせるコンピュータプログラムであって、

前記コンピュータを、先にランダム化させた画素値のずらし量に基づき、暗号化関数を用いて、ランダム化する画素値のずらし量を算出するスクランブル化手段として機能させることを特徴とするコンピュータプログラム

【請求項 21】

請求項 20 記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記暗号化関数の値の有効桁数に基づき、前記ランダム化する画素値のずらし量を調整することを特徴とするコンピュータプログラム。

【請求項 22】

請求項 20 記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、程度因子に基づき、前記ランダム化する画素値のずらし量を調整することを特徴とするコンピュータプログラム。

【請求項 23】

請求項 20 乃至 22 いずれか一項記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記先にランダム化した画素値のずらし量とパスワードとに基づき、前記ランダム化する画素値のずらし量を算出することを特徴とするコンピュータプログラム。

【請求項 24】

請求項 20 乃至 23 いずれか一項記載のコンピュータプログラムであって、

コンピュータを、前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段としてさらに機能させ、

前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とするコンピュータプログラム。

【請求項 25】

請求項 24 記載のコンピュータプログラムであって、

前記圧縮符号化手段としてのコンピュータは、J P E G 2 0 0 0 に基づき前記画像を圧縮符号化することを特徴とするコンピュータプログラム。

【請求項 26】

請求項 24 または 25 記載のコンピュータプログラムであって、

前記コンピュータを、前記画像のスクランブル化及び圧縮符号化に係る情報を電子透かしとして前記符号列に埋め込む電子透かし埋め込み手段としてさらに機能させることを特徴とするコンピュータプログラム。

【請求項 27】

請求項 20 乃至 26 いずれか一項記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記ランダム化する画素値の直前にランダム化した画素値のずらし量に基づき、前記ランダム化する画素値のずらし量を算出することを特徴とするコンピュータプログラム。

【請求項 28】

請求項 25 乃至 27 いずれか一項記載のコンピュータプログラムであって、

前記圧縮符号化手段として機能するコンピュータは、J P E G 2 0 0 0 の非可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、係数量子化手段の後に設けられ、量子化された離散ウェーブレット変換係数をランダム化することを特徴とするコンピュータプログラム。

【請求項 29】

請求項 25 乃至 27 いずれか一項記載のコンピュータプログラムであって、

前記圧縮符号化手段として機能するコンピュータは、J P E G 2 0 0 0 の可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、離散ウェーブレット変換手段の前に設けられ、画素値をランダム化することを特徴とするコンピュータプログラム。

【請求項 3 0】

コンピュータを、

請求項 2 0 乃至 2 9 のいずれか一項記載のコンピュータプログラムによりスクランブルされた符号データを J P E G 2 0 0 0 に基づき画像に復号化する、複数の過程よりなる復号化手段と、

前記復号化手段を構成する前記複数の過程の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、
として機能させることを特徴とするコンピュータプログラム。

【請求項 3 1】

請求項 2 0 乃至 3 0 のいずれか一項記載のコンピュータプログラムを格納している記憶媒体。

【書類名】 明細書

【発明の名称】 画像符号化装置、符号復号化装置、画像符号化方法、符号復号化方法、プログラム及び記憶媒体

【技術分野】**【0001】**

本発明は、画像符号化装置、符号復号化装置、画像符号化方法、符号復号化方法、プログラム及び記憶媒体に関する。

【背景技術】**【0002】**

近年、インターネットやパソコン等の普及・発展に伴い、インターネットを通じたデジタルデータの通信が幅広く行われるようになってきている。ここに、このようなデジタルデータの送信者は、そのデータを符号化して送信するようにしている。現に、プロバイダ等のデータ送信者（配布者）は、符号化された画像データを不特定多数の利用者に送信して配給するサービスを行っている。このようなサービスの一つとして、通信販売等における商品紹介に関するようなデータを、インターネットを通じて利用者に配信することが考えられる。この場合、プロバイダに対して予め料金を支払っている利用者（閲覧資格者）が、その支払った金額に応じて、受信した符号化データを復号して閲覧できるサービスである。

【0003】

しかしながら、このように不特定多数の人に符号化データを配信するサービスにおいては、閲覧資格者のみがその符号化データを正しく復号できなければ意味がない。かといって、将来、プロバイダと契約して閲覧資格者となる可能性のある一般ユーザが、その符号化された画像データを全く認識できないと、元々興味を引かず、その閲覧資格者数の増大を見込めない。

【0004】

このようなことから、この種の符号データに関しては、スクランブル処理した符号データとして配信する一方、閲覧資格者には復号時にスクランブルを解除するためのソフトウェア等を配布しておくことで、閲覧資格者は復号時にはスクランブルを解除して本来の正常な画像を閲覧できるようにするスクランブル方式が広く用いられている。このようにスクランブル処理することで、閲覧資格のないユーザは、本来の画像としては見にくかったり多少判りにくくなったりするが、逆に、本来の画像を見たくなる等の宣伝効果が生じ、閲覧資格者数の増大を見込めることとなる。

【0005】

このようなスクランブル方式に関しては、多数の提案例がある。そのうち、例えば、ラインローテーション、ラインバーミュテーション等のようにデータ列の並べ替えによって実現する方式と（例えば、特許文献1参照）、画像データのランダム化（乱数暗号化）によって実現する方式と、その他の方式（例えば、色空間軸の回転方式）等がある（これらについては、例えば、特許文献2参照）。

【特許文献1】 特開2001-218184号公報

【特許文献2】 特開2000-115581号公報

【発明の開示】**【発明が解決しようとする課題】****【0006】**

しかし、このような従来のスクランブル方法は、スクランブルするための情報をインデックス情報や位置補正量（パラメータ）などによって外部から入手することによって、又は平均値や直流値などの限られた固定値を選んで、スクランブルのための変動値（ Δ 変位）を決定しており、自由度の高い変動値を画像データ内部に保持することは難しかった。

【0007】

また、画像データにスクランブルをかけるにしても、画像データによってはスクランブルにより画像をかなり見にくくしたい場合やあまり見にくくしたくない場合等があるが、

その程度が一律であるため、プロバイダにおいて個々の画像データに応じて適切なレベルに画質を劣化させるスクランブル画像の提供が困難な現状にある。

【0008】

本発明の目的は、画像の画素値をランダム化して画像をスクランブルするとき、画像外部からの入力に頼らずに、自由度の高い変動値を確保することである。また、本発明の別の目的は、スクランブルにより画質が劣化する程度を自在に加減できるようにすることである。

【課題を解決するための手段】

【0009】

上記目的を達成するため、本発明の一態様に係る画像符号化装置は、画素値を順次ランダム化することにより画像をスクランブルする画像符号化装置であって、先にランダム化した画素値のずらし量に基づき、暗号化関数を用いて、ランダム化する画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする。

【0010】

画素値を順次ランダム化する場合に、先にランダム化した画素値のずらし量に基づき、後にランダム化する画素値のずらし量を決定するので、画像データに内在するランダム性を利用して、自由度の高い変動値を確保することができる。

【0011】

本発明の別の態様に係る画像符号化装置は、それぞれ暗号化関数の値の有効桁数を増減して画素値のずらし量を増減したり、ずらし基本量にかけられる程度因子を増減して画素値のずらし量を増減したりすることができる。

【0012】

本発明のさらに別の態様に係る画像符号化装置は、前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段をさらに備え、前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とする。

【0013】

スクランブル化手段は、複数の手段よりなる圧縮符号化手段の所定の段階に設け、スクランブル化手段が設けられた段階より後ろの手段はすべて可逆的であればよい。圧縮符号化手段は、例えば J P E G 2 0 0 0 に基づき画像を圧縮符号化することを特徴とする。J P E G 2 0 0 0 の係数量子化手段と可逆圧縮符号化手段の間に設けられた場合は、スクランブル化手段は量子化された離散ウェーブレット変換係数をランダム化する。また、J P E G 2 0 0 0 の離散ウェーブレット変換手段の前に設けられた場合は、スクランブル化手段は離散ウェーブレット変換前の画素値をランダム化する。ただし、この場合は、J P E G 2 0 0 0 での圧縮処理が全体で可逆機能（原画像が劣化無く復元できる）が選択されていなければならない。

【0014】

本発明のさらに別の態様に係る符号復号化手段は、上記の画像符号化装置によりスクランブルされた符号データを画像に復号化する、複数の手段よりなる復号化手段と、前記復号化手段を構成する前記複数の手段の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、を備えることを特徴とする。復号化手段におけるデスクランブル化手段は、画像符号化手段におけるスクランブル化手段の位置に対応する位置に設けられる。

【発明の効果】

【0015】

本発明に係る画像符号化装置は、画素値を順次ランダム化することにより画像をスクランブルする画像符号化装置であって、先にランダム化した画素値のずらし量に基づき、暗号化関数を用いて、ランダム化する画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする。したがって、画像の画素値をランダム化して画像をスク

ランブルする場合、画像外部からの入力に頼らずに、自由度の高い変動値を確保することができる。

【0016】

また、本発明の別の態様に係る画像符号化装置は、暗号化関数の値の有効桁数又は程度因子に基づき、画素値のずらし量を調整することができる。したがって、スクランブルにより画質が劣化する程度を自在に加減することができる。

【発明を実施するための最良の形態】

【0017】

本発明の一実施の形態を図面に基づいて説明する。

【0018】

【J P E G 2 0 0 0 について概略説明】

本実施の形態は、J P E G 2 0 0 0 アルゴリズムを利用するものであり、まず、J P E G 2 0 0 0 について概略説明する。

【0019】

図1は、J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを実現するシステムの機能ブロック図である。このシステムは、色空間変換・逆変換部101、2次元ウェーブレット変換・逆変換部102、量子化・逆量子化部103、エントロピー符号化・復号化部104、タグ処理部105の各機能ブロックにより構成されている。

【0020】

このシステムが従来のJ P E G アルゴリズムと比較して最も大きく異なる点の一つは変換方式である。J P E G では離散コサイン変換(D C T : Discrete Cosine Transform)を用いているのに対し、この階層符号化アルゴリズムでは、2次元ウェーブレット変換・逆変換部102において、離散ウェーブレット変換(D W T : Discrete Wavelet Transform)を用いている。D W T はD C T に比べて、高圧縮領域における画質が良いという長所を有し、この点が、J P E G の後継アルゴリズムであるJ P E G 2 0 0 0 でD W T が採用された大きな理由の一つとなっている。

【0021】

また、他の大きな相違点は、この階層符号化アルゴリズムでは、システムの最終段に符号形成を行うために、タグ処理部105の機能ブロックが追加されていることである。このタグ処理部105で、画像の圧縮動作時には圧縮データが符号列データとして生成され、伸長動作時には伸長に必要な符号列データの解釈が行われる。そして、符号列データによって、J P E G 2 0 0 0 は様々な便利な機能を実現できるようになった。例えば、ブロック・ベースでのD W T におけるオクターブ分割に対応した任意の階層(デコンポジション・レベル)で、静止画像の圧縮伸長動作を自由に停止させることができるようになる(後述する図3参照)。

【0022】

原画像の入出力部分には、色空間変換・逆変換101が接続される場合が多い。例えば、原色系のR(赤)/G(緑)/B(青)の各コンポーネントからなるR G B 表色系や、補色系のY(黄)/M(マゼンタ)/C(シアン)の各コンポーネントからなるY M C 表色系から、Y U V あるいはY C b C r 表色系への変換又は逆変換を行う部分がこれに相当する。

【0023】

次に、J P E G 2 0 0 0 アルゴリズムについて説明する。

【0024】

カラー画像は、一般に、図2に示すように、原画像の各コンポーネント111(ここではR G B 原色系)が、矩形をした領域によって分割される。この分割された矩形領域は、一般にブロックあるいはタイルと呼ばれているものであるが、J P E G 2 0 0 0 では、タイルと呼ぶことが一般的であるため、以下、このような分割された矩形領域をタイルと記述することにする(図2の例では、各コンポーネント111が縦横4×4、合計16個の矩形のタイル112に分割されている)。このような個々のタイル112(図2の例で、

R00, R01, ..., R15 / G00, G01, ..., G15 / B00, B01, ..., B15) が、画像データの圧縮伸長プロセスを実行する際の基本単位となる。従って、画像データの圧縮伸長動作は、コンポーネントごと、また、タイル112ごとに、独立に行われる。

【0025】

画像データの符号化時には、各コンポーネント111の各タイル112のデータが、図1の色空間変換・逆変換部101に入力され、色空間変換を施された後、2次元ウェーブレット変換部102で2次元ウェーブレット変換（順変換）が施されて、周波数帯に空間分割される。

【0026】

図3には、デコンポジション・レベル数が3の場合の、各デコンポジション・レベルにおけるサブバンドを示している。即ち、原画像のタイル分割によって得られたタイル原画像(0LL)（デコンポジション・レベル0）に対して、2次元ウェーブレット変換を施し、デコンポジション・レベル1に示すサブバンド(1LL, 1HL, 1LH, 1HH)を分離する。そして引き続き、この階層における低周波成分1LLに対して、2次元ウェーブレット変換を施し、デコンポジション・レベル2に示すサブバンド(2LL, 2HL, 2LH, 2HH)を分離する。順次同様に、低周波成分2LLに対しても、2次元ウェーブレット変換を施し、デコンポジション・レベル3に示すサブバンド(3LL, 3HL, 3LH, 3HH)を分離する。図3では、各デコンポジション・レベルにおいて符号化の対象となるサブバンドを、網掛けで表してある。例えば、デコンポジション・レベル数を3としたとき、網掛けで示したサブバンド(3HL, 3LH, 3HH, 2HL, 2LH, 2HH, 1HL, 1LH, 1HH)が符号化対象となり、3LLサブバンドは符号化されない。

【0027】

次いで、指定した符号化の順番で符号化の対象となるビットが定められ、図1に示す量子化・逆量子化部103で対象ビット周辺のビットからコンテキストが生成される。

【0028】

この量子化の処理が終わったウェーブレット係数は、個々のサブバンド毎に、「プレシント」と呼ばれる重複しない矩形に分割される。これは、インプリメンテーションでメモリを効率的に使うために導入されたものである。図4に示したように、一つのプレシントは、空間的に一致した3つの矩形領域からなっている。更に、個々のプレシントは、重複しない矩形の「コード・ブロック」に分けられる。これは、エントロピー・コーディングを行う際の基本単位となる。

【0029】

ウェーブレット変換後の係数値は、そのまま量子化し符号化することも可能であるが、JPEG2000では符号化効率を上げるために、係数値を「ビットプレーン」単位に分解し、画素あるいはコード・ブロック毎に「ビットプレーン」に順位付けを行うことができる。

【0030】

ここで、図5はビットプレーンに順位付けする手順の一例を示す説明図である。図5に示すように、この例は、原画像(32×32画素)を16×16画素のタイル4つで分割した場合で、デコンポジション・レベル1のプレシントとコード・ブロックの大きさは、各々8×8画素と4×4画素としている。プレシントとコード・ブロックの番号は、ラスタ順に付けられており、この例では、プレシントが番号0から3まで、コード・ブロックが番号0から3まで割り当てられている。タイル境界外に対する画素拡張にはミラーリング法を使い、可逆(5, 3)フィルタでウェーブレット変換を行い、デコンポジション・レベル1のウェーブレット係数値を求めている。

【0031】

また、タイル0 / プレシント3 / コード・ブロック3について、代表的な「レイヤ」構成の概念の一例を示す説明図も図5に併せて示す。変換後のコード・ブロックは、サブ

バンド (1LL, 1HL, 1LH, 1HH) に分割され、各サブバンドにはウェーブレット係数値が割り当てられている。

【0032】

レイヤの構造は、ウェーブレット係数値を横方向 (ビットプレーン方向) から見ると理解し易い。1つのレイヤは任意の数のビットプレーンから構成される。この例では、レイヤ0、1、2、3は、各々、1、3、1、3のビットプレーンから成っている。そして、LSB (Least Significant Bit: 最下位ビット) に近いビットプレーンを含むレイヤ程、先に量子化の対象となり、逆に、MSB (Most Significant Bit: 最上位ビット) に近いレイヤは最後まで量子化されずに残ることになる。LSBに近いレイヤから破棄する方法はトランケーションと呼ばれ、量子化率を細かく制御することが可能である。このように、ビットプレーン (又はサブビットプレーン) を削っていない状態の符号から所定の圧縮率になるまで符号を破棄する処理はポスト量子化と呼ばれており、JPEG2000アルゴリズムの最も大きな特徴である。

【0033】

図1に示すエントロピー符号化・復号化部104では、コンテキストと対象ビットから確率推定によって、各コンポーネント111のタイル112に対する符号化を行う。こうして、原画像の全てのコンポーネント111について、タイル112単位で符号化処理が行われる。最後にタグ処理部105は、エントロピー符号化・復号化部104からの全符号化データを1本の符号列データ (コードストリーム) に結合するとともに、それにタグを付加する処理を行う。

【0034】

図6には、この符号列データの1フレーム分の概略構成を示している。この符号列データの先頭と各タイルの符号データ (bit stream) の先頭にはヘッダ (メインヘッダ (Main header)、タイル境界位置情報やタイル境界方向情報等であるタイルパートヘッダ (tile part header)) と呼ばれるタグ情報が付加され、その後に、各タイルの符号化データが続く。なお、メインヘッダ (Main header) には、符号化パラメータや量子化パラメータが記述されている。そして、符号列データの終端には、再びタグ (end of codestream) が置かれる。

【0035】

一方、復号化時には、画像データの符号化時とは逆に、各コンポーネント111の各タイル112の符号列データから画像データを生成する。この場合、タグ処理部105は、外部より入力した符号列データに付加されたタグ情報を解釈し、符号列データを各コンポーネント111の各タイル112の符号列データに分解し、その各コンポーネント111の各タイル112の符号列データ毎に復号化処理 (伸長処理) を行う。このとき、符号列データ内のタグ情報に基づく順番で復号化の対象となるビットの位置が定められるとともに、量子化・逆量子化部103で、その対象ビット位置の周辺ビット (既に復号化を終えている) の並びからコンテキストが生成される。エントロピー符号化・復号化部104で、このコンテキストと符号列データから確率推定によって復号化を行い、対象ビットを生成し、それを対象ビットの位置に書き込む。このようにして復号化されたデータは周波数帯域毎に空間分割されているため、これを2次元ウェーブレット変換・逆変換部102で2次元ウェーブレット逆変換を行うことにより、画像データの各コンポーネントの各タイルが復元される。復元されたデータは色空間変換・逆変換部101によって元の表色系の画像データに変換される。

【0036】

〔画像符号化装置、符号復号化装置〕

本実施の形態の画像符号化装置、符号復号化装置は、その一例として、インターネット等のネットワークを利用してプロバイダから各ユーザに画像データ (デジタルコンテンツ) を配布するシステム構成を想定しており、配布元となるプロバイダのコンピュータを画像符号化装置、配布先となる各ユーザのコンピュータを符号復号化装置とする例である。

【0037】

図7はこのようなシステムを示す概略システム構成図であり、プロバイダの画像符号化装置となるサーバコンピュータ1にはインターネット等のネットワーク5を介して各ユーザの符号復号化装置となるパーソナルコンピュータ3が接続可能とされている。

【0038】

図8は、これらのサーバコンピュータ1やパーソナルコンピュータ3のハードウェア構成を概略的に示すブロック図である。図8に示すように、コンピュータ1、3は、当該コンピュータの主要部であって各部を集中的に制御するCPU (Central Processing Unit) 6を備えている。このCPU 6には、BIOSなどを記憶した読出し専用メモリであるROM (Read Only Memory) 7と、各種データを書換え可能に記憶するRAM (Random Access Memory) 8とがバス9で接続されている。RAM 8は、各種データを書換え可能に記憶する性質を有していることから、CPU 6の作業エリアとして機能し、例えば入力バッファ等の役割を果たす。

【0039】

さらにバス9には、HDD (Hard Disk Drive) 10と、配布されたプログラムであるコンピュータソフトウェアを読み取るための機構としてCD (Compact Disc) -ROM 11を読み取るCD-ROMドライブ12と、相手方となるコンピュータ3又は1とネットワーク5との通信を司る通信制御装置13と、キーボードやマウスなどの入力装置14と、CRT (Cathode Ray Tube) やLCD (Liquid Crystal Display) である表示装置15とが、図示しないI/Oを介して接続されている。

【0040】

そして、パーソナルコンピュータ3の場合であれば、ネットワーク5を介してサーバコンピュータ1からダウンロードした圧縮符号化された符号データは、HDD 10に格納されることになる。

【0041】

また、CD-ROM 11は、本発明の記憶媒体を実施するものであり、OS (Operating System) や各種コンピュータソフトウェアが記憶されている。CPU 6は、CD-ROM 11に記憶されているコンピュータソフトウェアをCD-ROMドライブ12で読み取り、HDD 10にインストールする。

【0042】

なお、記憶媒体としては、CD-ROM 11のみならず、DVDなどの各種の光ディスク、各種光磁気ディスク、FDなどの各種磁気ディスク等、半導体メモリ等の各種方式のメディアを用いることができる。また、通信制御装置13を介してインターネットなどのネットワーク5からコンピュータソフトウェアをダウンロードし、HDD 10にインストールするようにしてもよい。この場合に、送信側のサーバでコンピュータソフトウェアを記憶している記憶装置も、本発明の記憶媒体である。なお、コンピュータソフトウェアは、所定のOS (Operating System) 上で動作するものであってもよいし、その場合に後述の各種処理の一部の実行をOSに肩代わりさせるものであってもよいし、所定のアプリケーションソフトやOSなどを構成する一群のプログラムファイルの一部として含まれているものであってもよい。

【0043】

このような構成のコンピュータ1、3のHDD 10には、コンピュータソフトウェアの一つとして、画像を処理する画像処理プログラムが記憶されている。この画像処理プログラムは本発明のプログラムを実施するものである。そして、この画像処理プログラムに基づいてCPU 6が実行する処理により、コンピュータ1、3の各部の各種機能を実現する。その一つとして、図1を参照して説明したJPEG 2000アルゴリズムの各機能ブロックを備え、前述のようなJPEG 2000アルゴリズムにより画像データの圧縮符号化、又は、符号データの復号化を行う。即ち、図1に示したような圧縮符号化手段及び復号化手段の機能は、HDD 10に記憶されているプログラムに基づいてCPU 6が行う処理により実行される (もっとも、論理回路等を利用したハードウェア構成により実行させてもよい)。

【0044】

〔サーバコンピュータにおけるスクランブル画像符号化処理〕

前述したように、J P E G 2 0 0 0 アルゴリズムによれば、画像データの符号化に際しては、入力された画像データをウェーブレット変換した結果の離散ウェーブレット変換係数を量子化するまでは、可逆又は非可逆な変換過程をとることができ、量子化の処理が終わった離散ウェーブレット変換係数からエントロピー符号化等の符号列データを生成するまでは可逆変換過程となる。また、符号データの復号化に際して、入力された（圧縮保存済みの）符号列データから離散ウェーブレット変換係数データ（又は、量子化係数データ：可逆圧縮の場合は量子化しないため）を復号化するまでは、可逆変換過程を経ることとなり、復号化した離散ウェーブレット変換係数データから画像データを生成するまでは可逆又は非可逆な変換過程をとることができる。

【0045】

ここに、本実施の形態のサーバコンピュータ 1 は、例えば J P E G 2 0 0 0 アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとし、かつ、その圧縮符号化の際に必要な応じてスクランブル化処理を行って符号データを生成するものである。

【0046】

サーバコンピュータ 1 においてこのような画像符号化処理を行う J P E G 2 0 0 0 アルゴリズムによる圧縮符号化手段を適宜簡略化して書き直すと、図 9 (a) のように示すことができる。即ち、非可逆処理を離散ウェーブレット変換係数の量子化段階で行うものであり、スキャナ、デジタルカメラ、パソコン等の各種機器から処理対象となる画像データの入力を受付ける入力部 2 1、受付けた画像データに対して色空間変換等の処理を経た後、2次元ウェーブレット変換処理を行う2次元ウェーブレット変換部 2 2（102に相当）、変換された離散ウェーブレット変換係数に対して効率のよい圧縮を行うためにそのダイナミックレンジを削減するポスト量子化等の非可逆な量子化処理を行う係数量子化部 2 3（103に相当）、量子化された離散ウェーブレット変換係数に対して前述のエントロピー符号化（係数モデリング＋算術符号化）等の可逆圧縮符号化処理を行う可逆圧縮符号化部 2 4（104に相当）、符号化された符号データの並べ替え処理等を行い、必要箇所に出力する符号データ出力部 2 5（105に相当）による圧縮符号化手段 2 6 を有する。

【0047】

加えて、この圧縮符号化手段 2 6 により可逆圧縮符号化される直前のデータ、ここでは、係数量子化部 2 3 により量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段又はスクランブル化機能として作用するスクランブル化部 2 7 と、スクランブル化されたデータを復元するためのデータを電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み手段又は電子透かし埋め込み機能として作用する可逆電子透かし埋め込み部 2 8 とが付加されている。このようなスクランブル化部 2 7 は入力部 2 1 に対して画像データとともに所定のパスワード（英数字等による複数桁の暗証番号等）が入力された場合にのみ機能するものであり、入力されたパスワードは暗号化されてスクランブル化に供される。従って、画像データ入力に際してパスワードが入力されない場合には、スクランブル化部 2 7 及び可逆電子透かし埋め込み部 2 8 の処理を経ることなく、可逆圧縮符号化処理に移行する。

【0048】

J P E G 2 0 0 0 の準可逆圧縮においては、ウェーブレット変換部 2 2 及び係数量子化部 2 3 が通常非可逆過程となる。したがって、スクランブル化部 2 7 は、係数量子化部 2 3 と可逆圧縮符号化部 2 4 との間に設ければよい。図 9 (a) に示した一連の画像圧縮符号化過程において、スクランブル化部 2 7 より後段にある可逆電子透かし埋め込み部 2 8、可逆圧縮符号化部 2 4、出力部 2 5 はすべて可逆過程である。いずれかが非可逆であると、画像を再生するときに、スクランブルを解除できないからである。なお、非可逆電子透かし 2 8' を使用する場合は、図 9 (b) に示した通り、スクランブル化部 2 7 の前段に入れる必要がある。また、可逆電子透かし 2 8 及び非可逆電子透かし 2 8' を両方とも設けることも可能である。その場合は、図 9 (a) 及び (b) に示した位置にそれぞれ設

ければよい。

【0049】

ここで、スクランブル化部27での処理について説明する。このスクランブル化部27はランダム化によりデータのスクランブル化を行うものである。即ち、スクランブル前の元のデータに対して暗号化関数、例えばハッシュ (Hash) 関数に基づくハッシュ変換を施して乱数暗号化 (ランダム化) することにより、スクランブル前の元のデータを解読できないようにするものである。このハッシュ関数は、引数を種 (タネ) にして生成する一方向性の乱数発生関数であり、

性質1; 出力値から入力値は推測できない

性質2; 入力値が1ビットでも変わると、出力値は全面的に変化する

性質3; 同じ出力になる異なる2つの入力の探索は現実的には不可能

なる性質を有している (出典; 電子情報通信学会誌2000年2月“公平性保証とプライバシー保護”佐古和恵)。すなわち、ハッシュ関数とは、与えられた原文Xから固定長の擬似乱数Yを生成する関数 $Y = \text{Hash}(X)$ で、生成された値Yはハッシュ値と呼ばれる。値Yは値Xを種にした乱数とみなせるので、関数の計算方法を知らない者には値Yだけから値Xを推測することはできない。ハッシュ関数のこの性質を一方向性関数であるという。しかし、同じ値Xからは常に同じ値Yが算出される。逆ハッシュ関数 $X = \text{Hash}^{-1}(Y)$ が存在すれば、この逆変換関数によって、同じ値Yからは常に同じ値Xが算出される。また同じハッシュ値Yをもつ異なる原文Xを作成することは極めて困難である。

【0050】

このようにハッシュ変換は、生成後のデータから元のデータを推定することが不可能であるため、データのスクランブル化に際してハッシュ変換を用いることにより、その解読を防止することができる。

【0051】

電子透かし埋め込み部28による電子透かしの埋め込みは、スクランブル化されたデータを復号する際にパスワードを含む専用のソフトウェアにより元のデータへの復元を可能にするための処理であり、ここでは、スクランブルデータとスクランブル前のデータとの差分値 (ずらし量) を、ハッシュ関数を用いたランダム化で復元できるように暗号化した電子透かしデータとして、画像全体のスクランブル後のデータ (ここでは、量子化・スクランブル化された離散ウェーブレット変換係数) 中に埋め込むものである。

【0052】

ここで、本実施の形態で使用する暗号化関数を簡単に説明する。本実施の形態の暗号化関数には、以下のハッシュ変換を用いる。

【0053】

$$[\text{変換結果データ}] = [\text{変換元データ}] * [\text{生成元}] \% [\text{法: 素数}] \quad (\text{式1})$$

(式1) は、変換元データに生成元を掛け、所定の素数を法とする剰余を変換結果データとするものである。逆変換は以下の通りとなる。

【0054】

[変換元データ]

$$= ([\text{変換結果データ}] + [\text{法: 素数}] * m) \text{ l.c.m. } [\text{生成元}] / [\text{生成元}] \quad (\text{式2})$$

(式2) は、変換結果データにm倍の素数を足したものと生成元との最小公倍数を、生成元で割ったものを変換元データとするものである。ここで、A l.c.m. B は、整数Aと整数Bとの最小公倍数 (Lowest Common Multiple) を表す。また、以上の式1、式2内の生成元は、同じ値の整数によるべき乗 (例えば、生成元の二乗や三乗) したものに置換えても良い。

【0055】

例えば、変換元データ: 101、生成元: 3、法: 127とした場合、上記のハッシュ変換により変換元データは

$$\text{変換結果データ} = 101 * 3 \% (\text{法: } 127) = 49$$

に変換される。また、逆変換により変換結果データは

変換元データ

$$= ([49] + [\text{法}:127] * m) \text{ l.c.m. } [\text{生成元}:3] / [\text{生成元}:3] = 101 \dots m=2 \text{ であるので、l.c.m.} = 303 \text{ となることによる}$$

に変換され、変換元データが復元される。

【0056】

上記のハッシュ変換を利用して、本実施の形態の暗号化関数 $Y = \text{Hash}(X)$ を以下の通り定義する。

【0057】

[X: 10進数]	[Y: 8桁の2進数]
0	: 11111111
1 ~ 126	: 先頭1bitはON “1” とし、後続の7bitは 変換前データ X (1 ~ 126) をハッシュ変換した 結果を2進数としたデータ
127	: 10000000
128	: 01111111
129 ~ 254	: 先頭1bitはOFF “0” とし、後続の7bitは 変換前データ X (129 ~ 254) から128を引き、 ハッシュ変換した結果を2進数としたデータ
255	: 00000000

上記の暗号化関数により、変換前データ 0 ~ 255 を8桁の2進数 00000000 ~ 11111111 (または2桁の16進数) で乱数化でき、異なる変換前データ X には異なる変換後データ Y を対応させることができる。

【0058】

上記の暗号化関数の具体例を示す。変換前後のデータはすべて2桁ずつに区切り、16進数とみなして上記の暗号化関数を適用している。

【0059】

[法: 素数] = 127 (10進数)

[生成元] = 3

[変換元データ] = 20010831 (8桁の16進数とみなし、2桁ずつに区切って上記の暗号化関数を適用する)

< [変換結果データ] 使用の変換 >

変換後data: E0839894

< [変換結果データ] $^{-1}$ 使用の変換 >

変換後data: B5D5ADE5

[逆変換後データ] = 20010831 (日付: 2001年8月31日) となり、復元される。

【0060】

暗号化の方法 (暗号化関数) としては、ハッシュ変換を使用するもの以外に、周知の RSA などの公開鍵方式を利用してもよいし、DES、AES等の共通鍵暗号方式を利用してもよい。

【0061】

本実施の形態の暗号化関数を用いて画像をスクランブル化処理する場合、暗号化前後における画素値のずらし量 (差分値) を決定する方法について説明する。

【0062】

いま、画素値のずらし量の算出の基礎となるずらし基本量を R_k 、ずらし方向を P_k とし、

$R_k = \text{Hash}(\text{“パスワード”}, \text{“直前}(k-1)\text{番目の処理済値”})$ の

最下位ビットを除いた値

$P_k = \text{Hash}(\text{“パスワード”}, \text{“直前}(k-1)\text{番目の処理済値”})$ の

最下位ビットがONの場合 “-1”、OFFの場合 “+1”

とする。ここで、処理済値とは、画素 (画素の並び) を順次処理する場合における直前の

処理結果（ずらし基本量）である。別の実施形態においては、処理済値として、直前の処理結果でなく、より先の処理結果（例えば $k-2$ 番目、 $k-3$ 番目）を使用してもよいし、複数の処理結果（例えば $k-1$ 番目と $k-2$ 番目の両方）を使用してもよい。

【0063】

このように、暗号化関数 $Hash$ の値の最下位ビットを除いた値をとることにより、すなわち、有効桁数を増減することにより、ずらし基本量 R_k の増減範囲を調整することができる。

【0064】

暗号化関数の引数として“パスワード”が含まれているが、これは“パスワード”と“直前（ $k-1$ ）番目の処理済値”とで決まる値に対して、暗号化関数 $Hash(X)$ を適用することを意味する。

【0065】

ずらし基本量 R_k をそのままランダム化する画素のずらし量としてもよい。すなわち

$$(\text{ずらし量}) = R_k * P_k$$

また、程度因子を導入して、ずらし量を

$$(\text{ずらし量}) = R_k * (\text{程度因子}) * P_k$$

で算出してもよい。程度因子とは、ずらし基本量 R_k に掛ける倍率である。程度因子が大きいほどずらし量が大きくなり、画像をスクランブルする程度が高くなる。逆に程度因子が小さいほどずらし量が小さくなり、画像をスクランブルする程度が低くなる。

【0066】

図10に具体的な数値例を示す。図10において、(1)は処理順序 $No.$ 、(2)は元の量子化データ、(3)はスクランブル用増減値（＝ずらし量） $= R_k * (\text{程度因子}: 2) * P_k$ である。図10を参照して、 k 番目の画素のずらし量の算出を説明する。 $k-1$ 番目の画素値は11、画素のずらし量は $R(k-1) * \text{程度因子} = (+2) * 2$ であるから、

$R_k = Hash(\text{“パスワード”, } (11+2*2))$ の最下位ビットを除いた値、

$P_k = Hash(\text{“パスワード”, } (11+2*2))$ の最下位ビットがONの場合“−1”、OFFの場合“+1”

となる。ここで、 $Hash(\text{“パスワード”, } (11+2*2)) = 7$ （10進数） $= 111$ （2進数）であると仮定すると、

$$R_k = 11 \text{（2進数）} = 3 \text{（10進数）}$$

$$P_k = -1 \text{（最下位ビットがON“1”）}$$

$$(\text{ずらし量}) = 3 * (\text{程度因子}: 2) * (-1) = -6$$

となる。

【0067】

ここで、程度因子は例として“2”を使用しているが、この値は、スクランブル化時に、固定値で透かしデータにして符号化された画像に埋め込んでおいてもよいし、また、スクランブル化及びデスクランブル化する時にユーザが入力するようにしてもよい。

【0068】

本実施形態においては、暗号化関数値の最下位ビットを P_k 、最下位ビットを除いたビットを R_k として使用している。別の実施形態においては、 P_k はどのビットを使用して決定してもよいし、複数のビットに基づき決定してもよい。また、 R_k は暗号化関数値から P_k に使用したビットを除いてもよいし、除かなくてもよい。

【0069】

このように離散ウェーブレット変換係数はスクランブル化され、復元のための暗号化された電子透かしデータが埋め込まれたデータ（離散ウェーブレット変換係数）に対して可逆圧縮符号化部24によって可逆変換を施すことにより、スクランブル化され、かつ、電子透かしデータが埋め込まれた離散ウェーブレット変換係数を劣化させることなく圧縮させることができる。この後、タグ処理等が施された符号データは、HDD10等のメモリに保存される。

【0070】

このように、本実施の形態によれば、サーバコンピュータ 1 において、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後の圧縮符号化処理は可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後の量子化された離散ウェーブレット変換係数にスクランブルをかけても、データを劣化させることなく圧縮させることができるので、そのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすことが可能となる。そして、このようなスクランブルデータを元のデータに復元するためのデータが暗号化された電子透かしデータとして画像全体に埋め込まれているので、不特定多数の利用者によるスクランブル解除のための解読を事実上不可能にし、スクランブル前の元データの保護を図ることができる。

【0071】

ところで、スクランブル化部 27 で乱数暗号化するデータの対象としては、離散ウェーブレット変換係数の最上位係数を避け、下位係数を主体に行うことが望ましい。上位係数ほど元の画像データに近いものであり、このような係数を対象にランダム化すると、暗号化の程度が大きくなり、スクランブル画像から元の画像を全く想像できなくなってしまうからである。もっとも、最上位係数しかない場合には、最上位係数を乱数暗号化の対象とする。

【0072】

より具体的には、量子化としてビットプレーン化されたビット係数（離散ウェーブレット変換係数）の有意係数を対象としてスクランブル化すればよい。「ビット係数の有意係数」とは、例えば前述の J P E G 2 0 0 0 アルゴリズム中で説明したようにビット表現した処理対象となるビットプレーン化された離散ウェーブレット変換係数を上位ビットから下位ビット方向に符号化する場合に、注目するビット係数が 0 でないことが判っている係数をいう。このようなビットプレーン化されたビット係数の有意係数を対象としてスクランブル化することで、効果的なスクランブルをかけることができる。

【0073】

この場合のスクランブル化処理例として、対象となるビット係数を反転させる方式（“0”→“1”に反転、又は、“1”→“0”に反転）を採用することができる。このようなビット係数反転方式を採用する場合、その隣り桁（直上桁又は直下桁）のビット係数も併せて反転させることが望ましい。即ち、“0”→“1”に反転であれば、“1”→“0”に反転し、“1”→“0”に反転であれば、“0”→“1”に反転する。これは、スクランブル化により対象となるビット係数を反転させる場合には、そのビット係数の反転処理よりこの部分で極端に表示画像の明るさが変わってしまい画質劣化することがあるので、この画質劣化への影響を軽減・緩和させるためである。もっとも、この場合もあまりスクランブルをかけすぎると元の画像が判らなくなってしまうので、このような場合には、直下桁側の隣り桁のみ反転させることが望ましい。

【0074】

また、スクランブル化部 27 による量子化データ（離散ウェーブレット変換係数）のスクランブル処理に際しては、J P E G 2 0 0 0 の特徴を利用することにより、そのスクランブルレベル（従って、画質劣化レベル）を任意に可変設定することができるので、プロバイダが提供する画像データの目的・用途に応じて適宜スクランブルレベルを設定することにより、画質劣化レベルを加減したスクランブル画像を提供することができる。

【0075】

図 11 は、程度因子を変化させてスクランブルの程度を変えた場合を示す図である。はっきりした元画像と比較して、スクランブルをかけた画像は乱れているが、その乱れ方の程度はスクランブルの掛け方、すなわち程度因子の大小により異なることがわかる。スクランブルは可逆変換なので、スクランブルを解除すれば、元画像を完全に再現することが可能である。

【0076】

このようなスクランブルレベルを可変設定する一例としては、J P E G 2 0 0 0 アルゴリズムにおける図 5 中に示したようなビットプレーン処理を利用することができる。つまり、J P E G 2 0 0 0 アルゴリズムによれば、画像データの閲覧に際してサブバンド機能等を利用することでサムネイル画像の提供が簡単に行えるが、例えば、ビットプレーンにおけるビット係数の上位ビットのデータをランダム化によりスクランブルをかければ、解像度は変わらない状態で画像の形が崩れることによりボケたようなスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、ビットプレーンにおけるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在となる。

【0077】

スクランブルレベルを可変設定する他例としては、J P E G 2 0 0 0 アルゴリズムの離散ウェーブレット変換処理によるサブバンド構造を利用することができる。J P E G 2 0 0 0 アルゴリズムによれば、解像度に関して図 3 等に示したようなサブバンド階層構造を有し、低階層の L L (3 L L , 2 L L , 1 L L 等) なるサブバンドが最も解像度の高い部分となるので、例えば、低階層のサブバンド部分のデータをランダム化によりスクランブルをかければ、繊細なスクランブル、即ち、サムネイル画像への画質劣化の影響を与えにくいスクランブルを実現できる。よって、離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在となる。

【0078】

スクランブルレベルを可変設定するさらに他例としては、J P E G 2 0 0 0 アルゴリズムにおける処理単位を利用することができる。J P E G 2 0 0 0 アルゴリズムによれば、図 4 等で前述したように、画像全体に限らず、符号化単位となる複数の矩形領域 (タイル) を単位として処理が可能であるので、例えば、ランダム化によるスクランブル化を行う領域を限定するブロックの大きさを大きくすると、雑然としたスクランブル画像となり、画像中で表現される元の形 (画像全体像) が判り難くなるスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、スクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在となる。

【0079】

[パーソナルコンピュータにおけるスクランブル符号復号化処理]

本実施の形態のパーソナルコンピュータ 3 は、プロバイダであるサーバコンピュータ 1 から配布される符号データを J P E G 2 0 0 0 アルゴリズムの非可逆モードにより復号化するものとし、かつ、プロバイダにより閲覧許可されたユーザであれば、復号時にスクランブルを解除するためのパスワードを含むソフトウェアの配布を受けており、その復号化の際にパスワード入力により電子透かしデータを解読してデスクランブル化処理を行って元の画像データを復元するものである。

【0080】

パーソナルコンピュータ 3 においてこのような符号復号化処理を行う J P E G 2 0 0 0 アルゴリズムによる復号化手段を適宜簡略化して書き直すと、図 1 2 のように示すことができる。即ち、サーバコンピュータ 1 からネットワーク 2 を通じて配布される前述のようにスクランブル化された符号データの入力を受付ける符号データ入力手段又は符号データ入力機能として作用する入力部 3 1 に対して、受付けた符号データに対してエントロピー復号化処理等の可逆圧縮符号の復号化処理を行う可逆圧縮符号の復号化部 3 2、2 次元ウェーブレット逆変換等を行って元の画像データに復元する 2 次元ウェーブレット逆変換部 3 3 (1 0 3 , 1 0 2 , 1 0 1 等に相当) による復号化手段 3 4 を有する。

【0081】

加えて、復号化部 3 2 と 2 次元ウェーブレット逆変換部 3 3 との間には、符号データ中に埋め込まれている電子透かしデータを解読するための可逆電子透かし解読部 3 5 と、解読された電子透かしデータに基づき符号データのスクランブルを解除するデスクランブル化手段又はデスクランブル化機能として作用するスクランブル解除部 3 6 とが付加されて

いる。このような電子透かし解読部 35 やスクランブル解除部 36 は、入力部 31 に対して符号データとともに所定のパスワードが入力された場合のみ機能するものであり、入力されたパスワードに基づき電子透かし解読部 35 で符号データ中に埋め込まれている電子透かしデータを解読し、解読された電子透かしデータ中の差分値データ等に基づきスクランブル解除部 36 で符号データのスクランブルを解除する。従って、プロバイダから閲覧許可されてそのための専用ソフトが配給されていない通常の J P E G 2 0 0 0 アルゴリズムのみの復号化ソフトによる復号処理では、スクランブル化され、かつ、所定の電子透かしデータが埋め込まれて配布される符号データを解読・デスクランブル化することができず、スクランブル化された符号データを元の画像データに復元することはできない。

【0082】

前述のハッシュ変換を用いたスクランブル化処理時の元のデータからのずらし量（差分値）の決定方法に対応する、パーソナルコンピュータ 3 側での復号時の戻し量の決定方法の、具体的な例について説明する。

【0083】

いま、

$R_k = \text{Hash}(\text{“パスワード”}, \text{“復元前の直前}(k-1)\text{番目の量子化データ値”})$
の最下位ビットを除いた値

$P_k = \text{Hash}(\text{“パスワード”}, \text{“復元前の}(k-1)\text{番目の量子化データ値”})$ の
最下位ビット \rightarrow ON: $\ast(-1)$ 、OFF: $\ast(+1)$

とすると（ P_k に関する式中の復元前の量子化データ値とは、順次処理（画素の並び）における直前の量子化データの復元前データ（ずらし状態のままの量子化データ）である）

$(\text{戻し量}) = -(\text{ずらし量}) = R_k \ast (\text{程度因子}) \ast P_k \ast (-1)$

で表される。具体的な数値例を示すと、前述の図 10 に示すような量子化データの並びの場合、前述のずらし量決定の場合と同様に、

$R_k = 3$ （最下位ビットを除いた値）

$P_k = -1$ （最下位ビットが ON）

$(\text{戻し量}) = -(\text{ずらし量}) = 3 \ast (\text{程度因子: } 2) \ast (-1) \ast (-1) = +6$

となる。

【0084】

[変形例]

図 9 (a) では、サーバコンピュータ 1 が、例えば J P E G 2 0 0 0 アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとして説明したが、J P E G 2 0 0 0 アルゴリズムの可逆モードにより画像データを圧縮符号化する場合であれば、図 13 (a) に示すように、スクランブル化部 27 及び可逆電子透かし埋め込み部 28 を 2 次元ウェーブレット変換部 22 の前段に設け、離散ウェーブレット変換処理前の画像データをスクランブル化し、かつ、電子透かしデータを埋め込むようにしてもよい。なお、可逆ウェーブレット変換部 22' 及び可逆係数量子化部 23' は、図 9 (a) のウェーブレット変換部 22 及び係数量子化部 23 に対応する。

【0085】

即ち、入力された画像データを J P E G 2 0 0 0 アルゴリズムの可逆モードに従い圧縮符号化する場合であれば、離散ウェーブレット変換処理前の画像データであっても可逆的に完全に復号されるので、この時点の画像データにスクランブルをかけ、かつ、電子透かしデータを埋め込んでも、可逆的に完全に復号させることができるからである。図 13 (b) に示した通り、非可逆電子透かし 28' を使用する場合は、スクランブル化部 27 より前段（例えば、入力部 21 とスクランブル化部 27 の間）に入ればよい。

【産業上の利用可能性】

【0086】

画像の画素値をランダム化して画像をスクランブルするとき、画像外部からの入力に頼らずに、自由度の高い変動値を確保することができ、スクランブルの程度を自在に変更

できる画像符号化装置を提供することができる。

【図面の簡単な説明】

【0087】

【図1】本発明の前提となる J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを実現するシステムの機能ブロック図である。

【図2】原画像の各コンポーネントの分割された矩形領域を示す説明図である。

【図3】デコンポジション・レベル数が3の場合の、各デコンポジション・レベルにおけるサブバンドを示す説明図である。

【図4】プレシントを示す説明図である。

【図5】ビットプレーンに順位付けする手順の一例を示す説明図である。

【図6】符号列データの1フレーム分の概略構成を示す説明図である。

【図7】本発明の一実施の形態のシステムを示すシステム構成図である。

【図8】コンピュータのハードウェア構成を概略的に示すブロック図である。

【図9】サーバコンピュータにおける画像圧縮符号化の処理系を書き直して示す機能的ブロック図である。

【図10】スクランブル化によるずらし量の算出方法を説明するための表である。

【図11】スクランブル化した画像の例を示す図である。

【図12】パーソナルコンピュータにおける符号復号化の処理系を書き直して示す機能的ブロック図である。

【図13】サーバコンピュータにおける画像圧縮符号化の処理系の変形例を示す機能的ブロック図である。

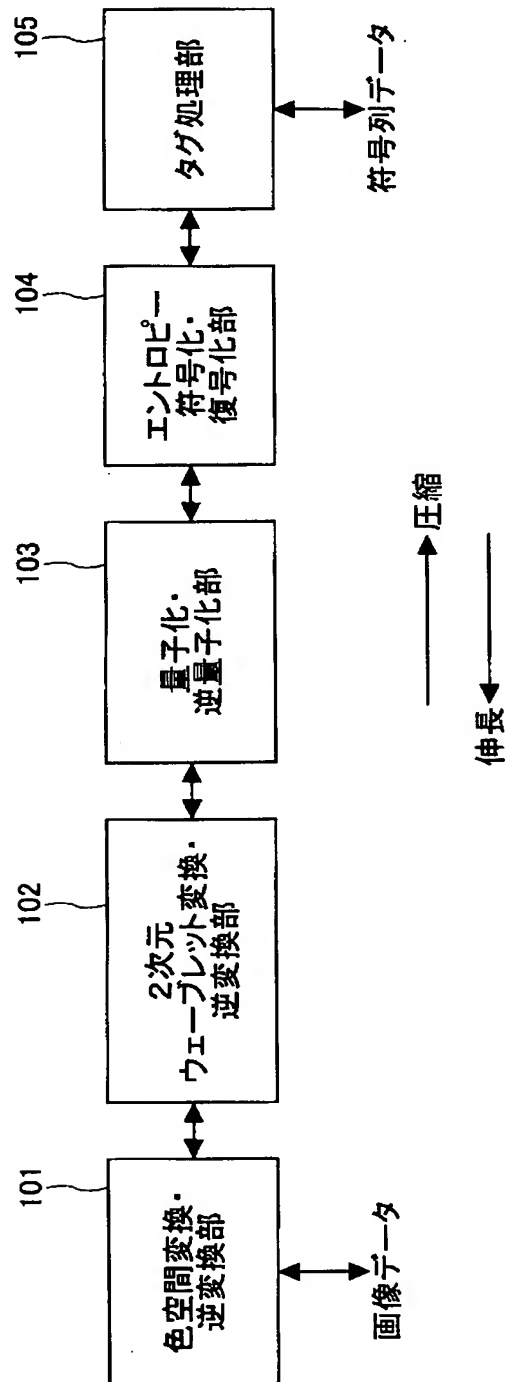
【符号の説明】

【0088】

- | | |
|----|-------------------------|
| 1 | 画像符号化装置 |
| 3 | 符号復号化装置 |
| 26 | 圧縮符号化手段、圧縮符号化機能 |
| 27 | スクランブル化手段、スクランブル化機能 |
| 28 | 電子透かし埋め込み手段、電子透かし埋め込み機能 |
| 31 | 符号データ入力手段、符号データ入力機能 |
| 34 | 復号化手段、復号化機能 |
| 36 | デスクランブル化手段、デスクランブル化機能 |

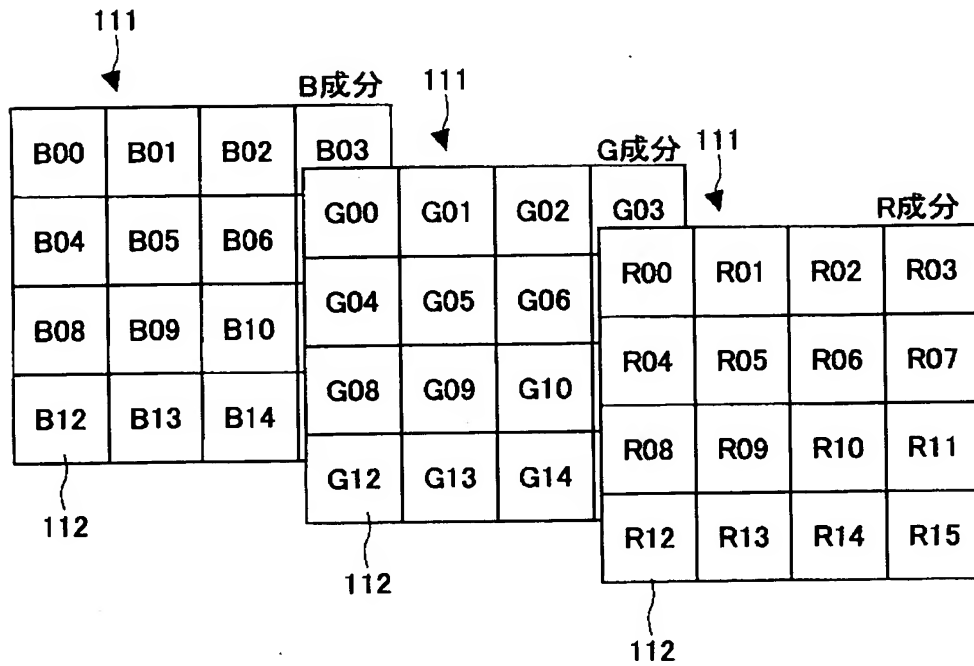
【書類名】 図面
【図 1】

本発明の前提となる J P E G 2 0 0 0 方式の基本となる
階層符号化アルゴリズムを実現するシステムの機能ブロック図



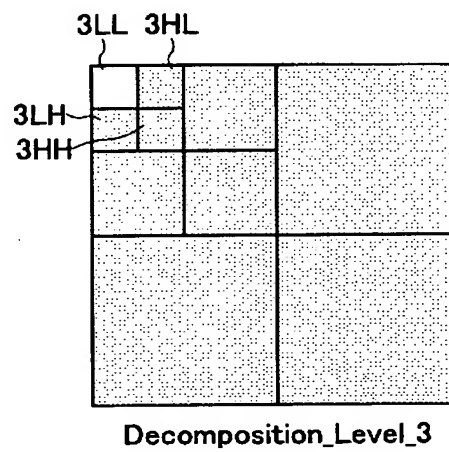
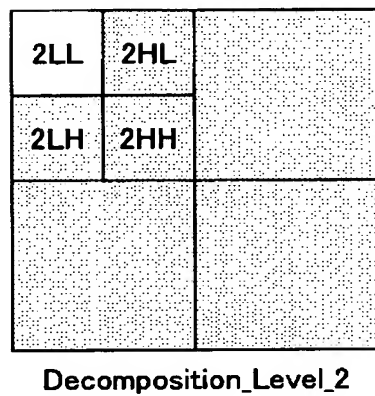
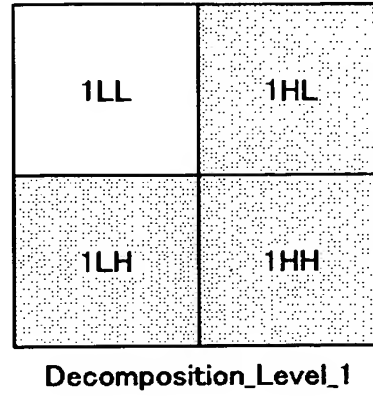
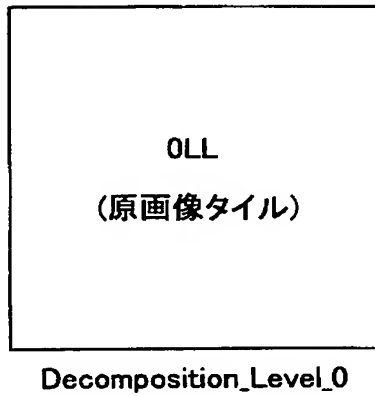
【図 2】

原画像の各コンポーネントの分割された矩形領域を示す説明図



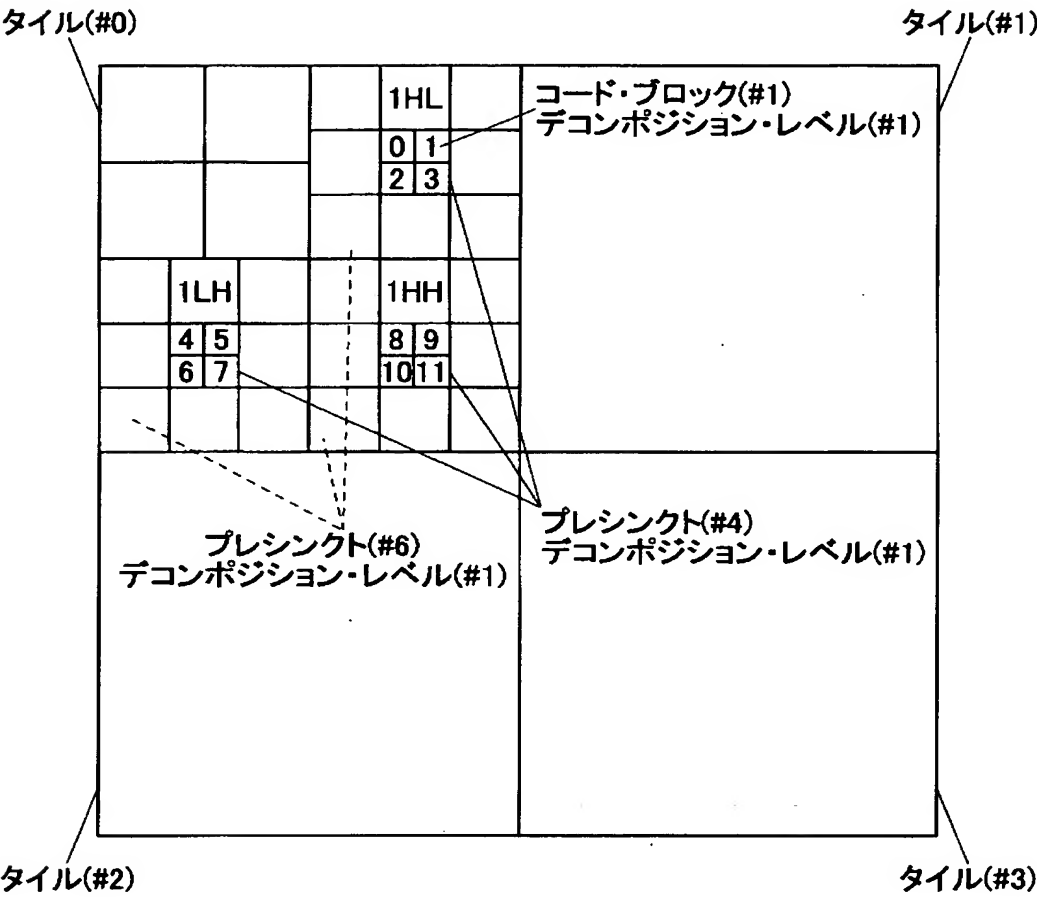
【図 3】

デコンポジション・レベル数が3の場合の、
各デコンポジション・レベルにおけるサブバンドを示す説明図



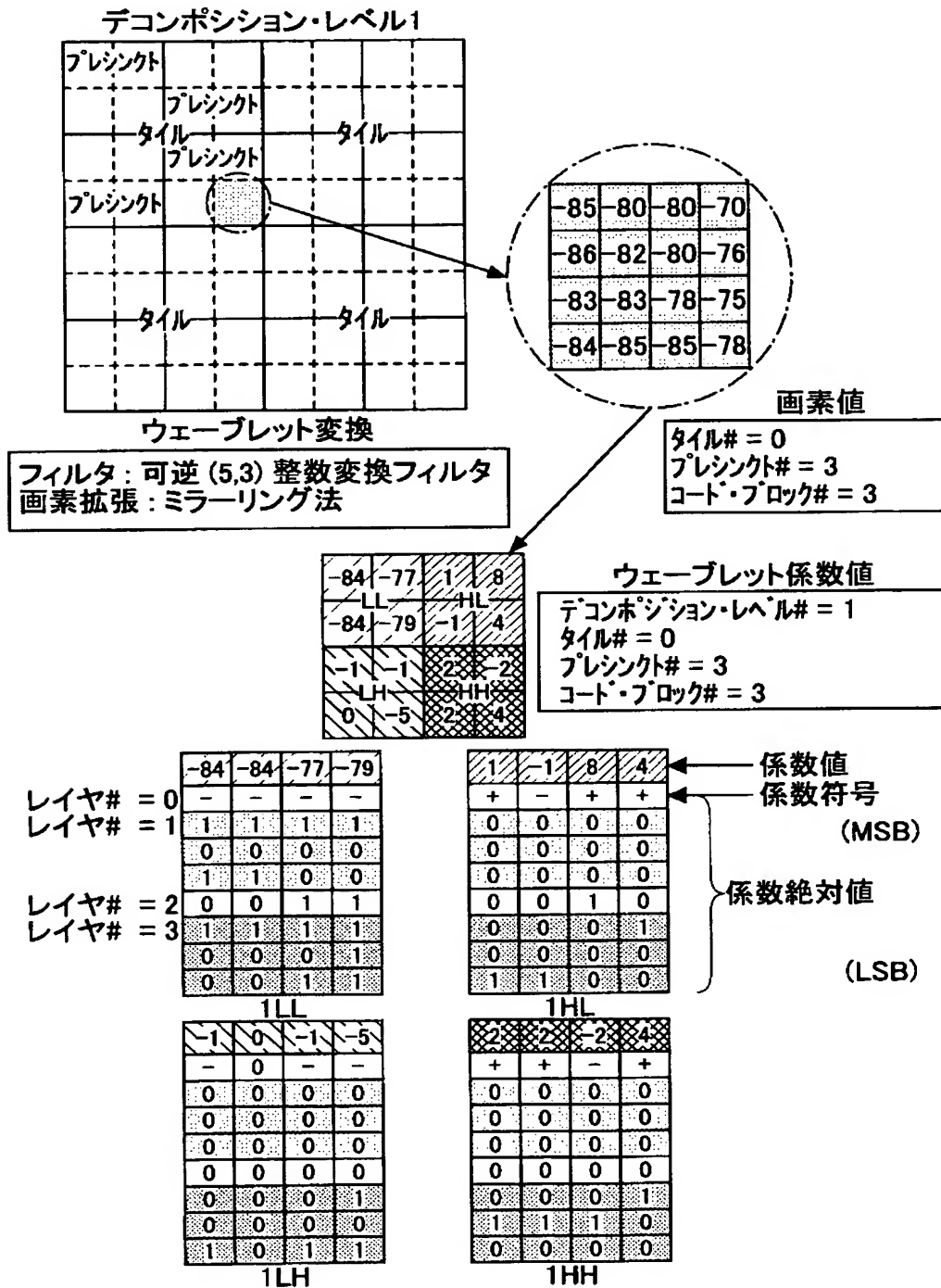
【図 4】

プレシントを示す説明図



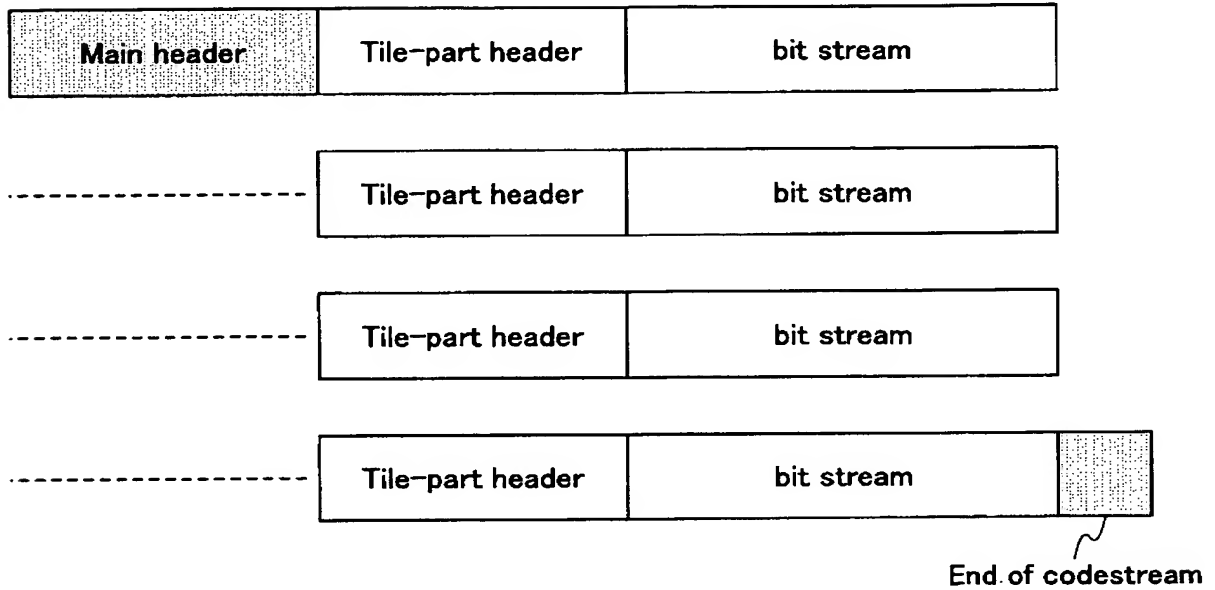
【図 5】

ビットプレーンに順位付けする手順の一例を示す説明図



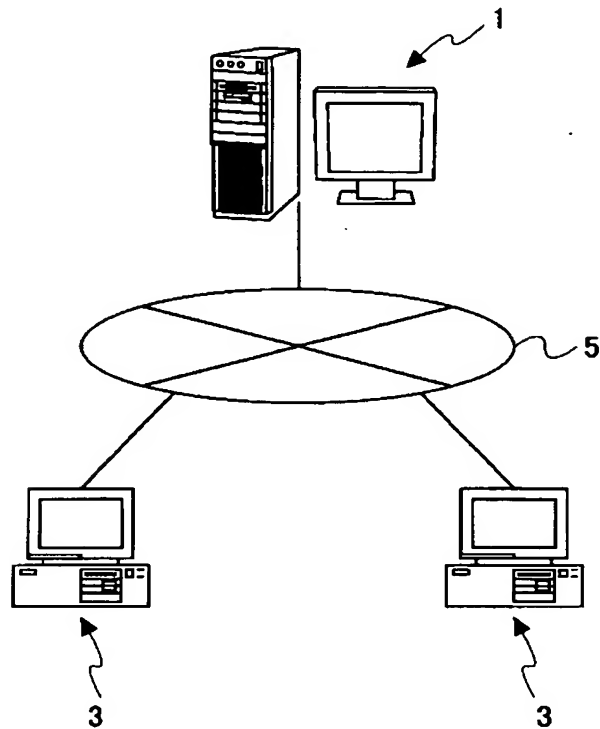
【図 6】

符号列データの 1 フレーム分の概略構成を示す説明図



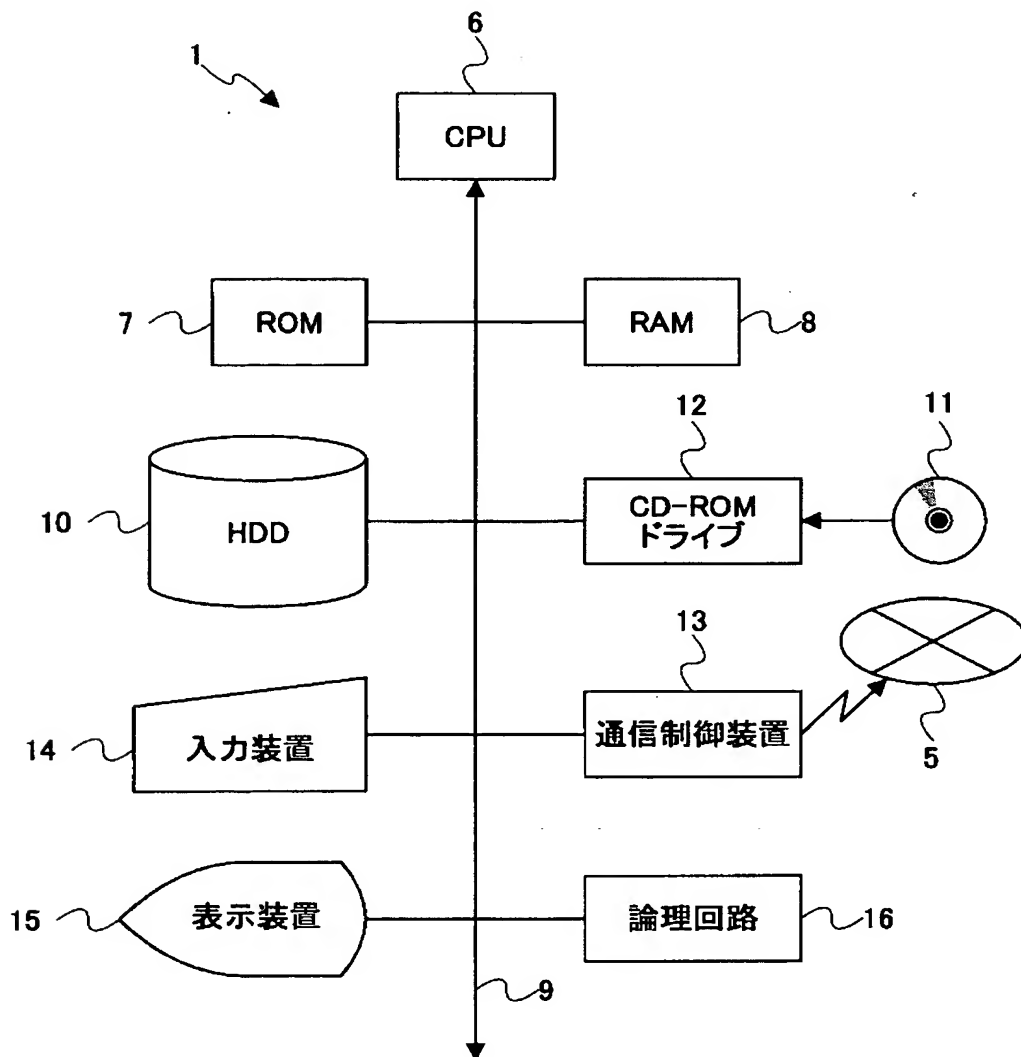
【図 7】

本発明の一実施の形態のシステムを示すシステム構成図



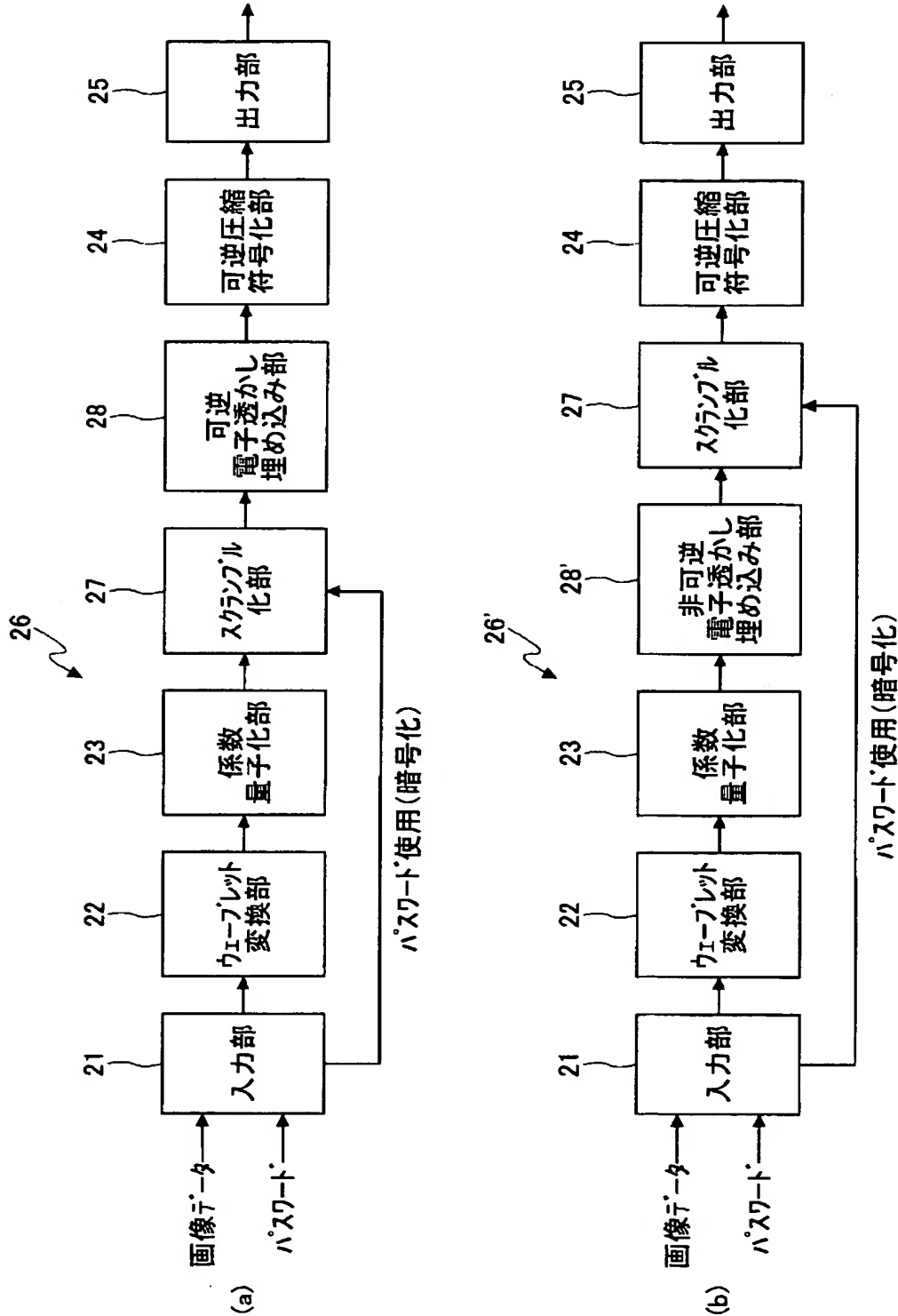
【図 8】

コンピュータのハードウェア構成を概略的に示すブロック図



【図 9】

サーバコンピュータにおける画像圧縮符号化の
処理系を書き直して示す機能的ブロック図



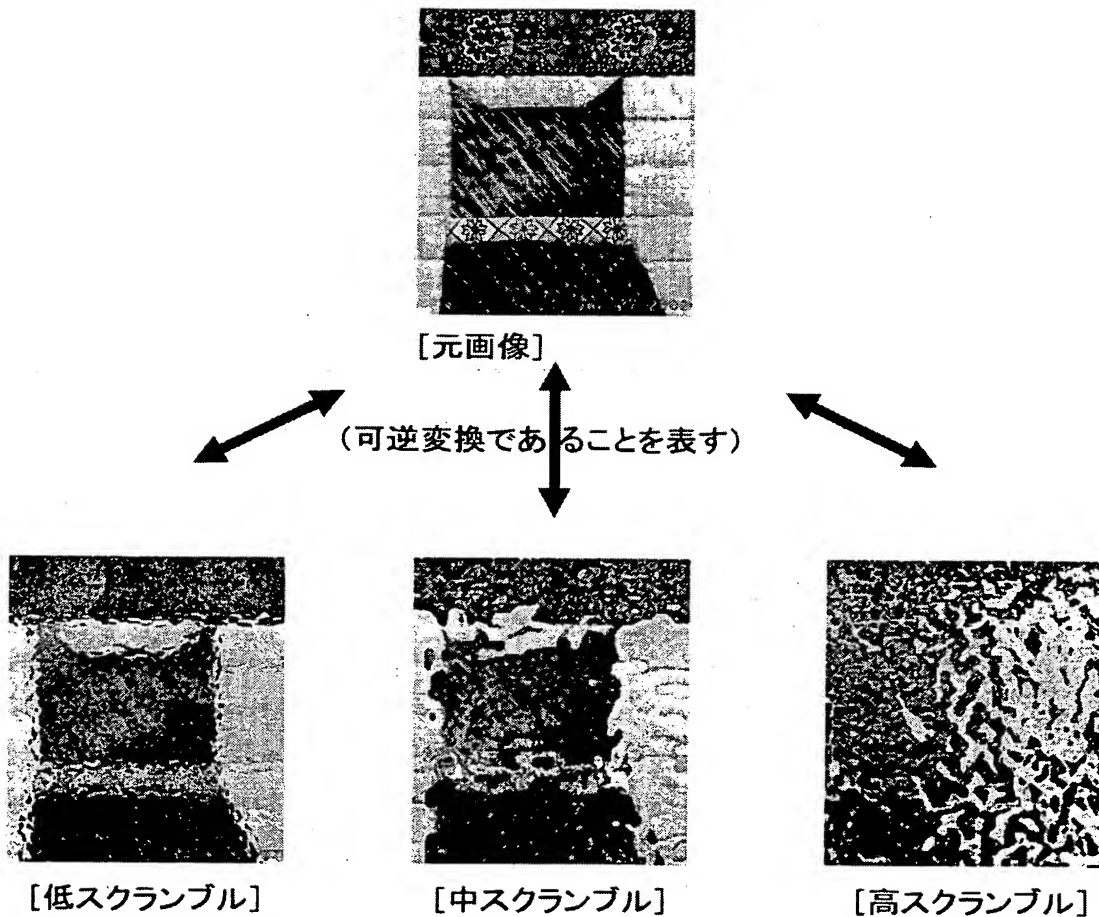
【図 10】

スクランブル化によるずらし量の算出方法を説明するための表

(1)	$k-1$	k	$k+1$	$k+2$
(2)	11	19	23	20
(3)	$(+2)*2$	$(-3)*2$	$(-1)*2$	$(+1)*2$

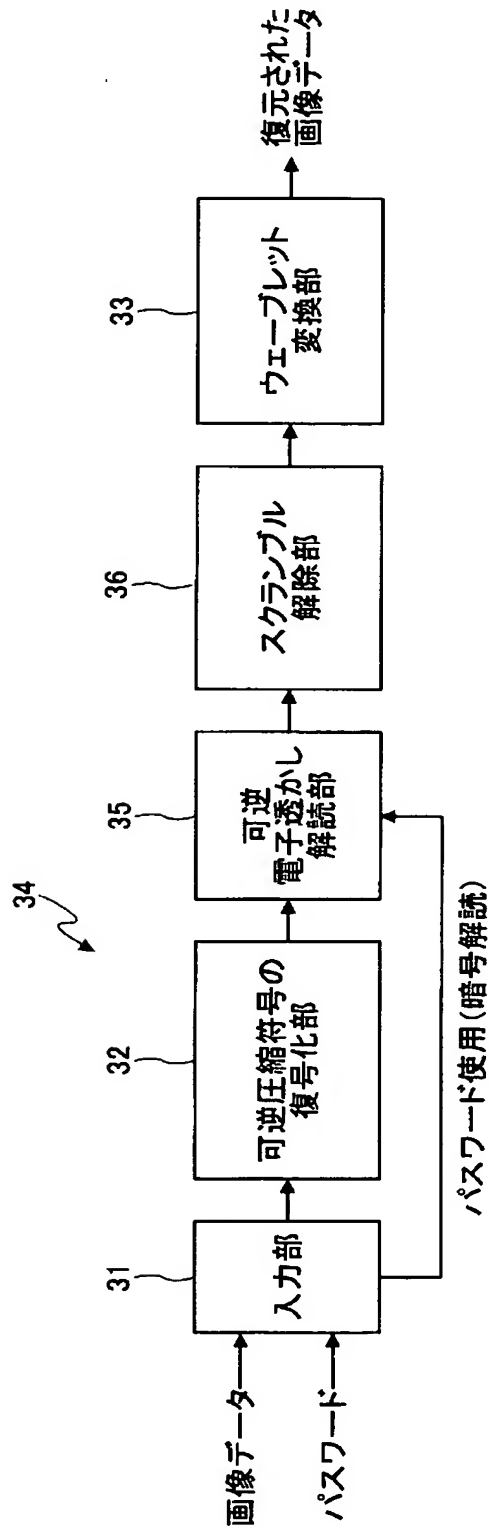
【図 11】

スクランブル化した画像の例を示す図



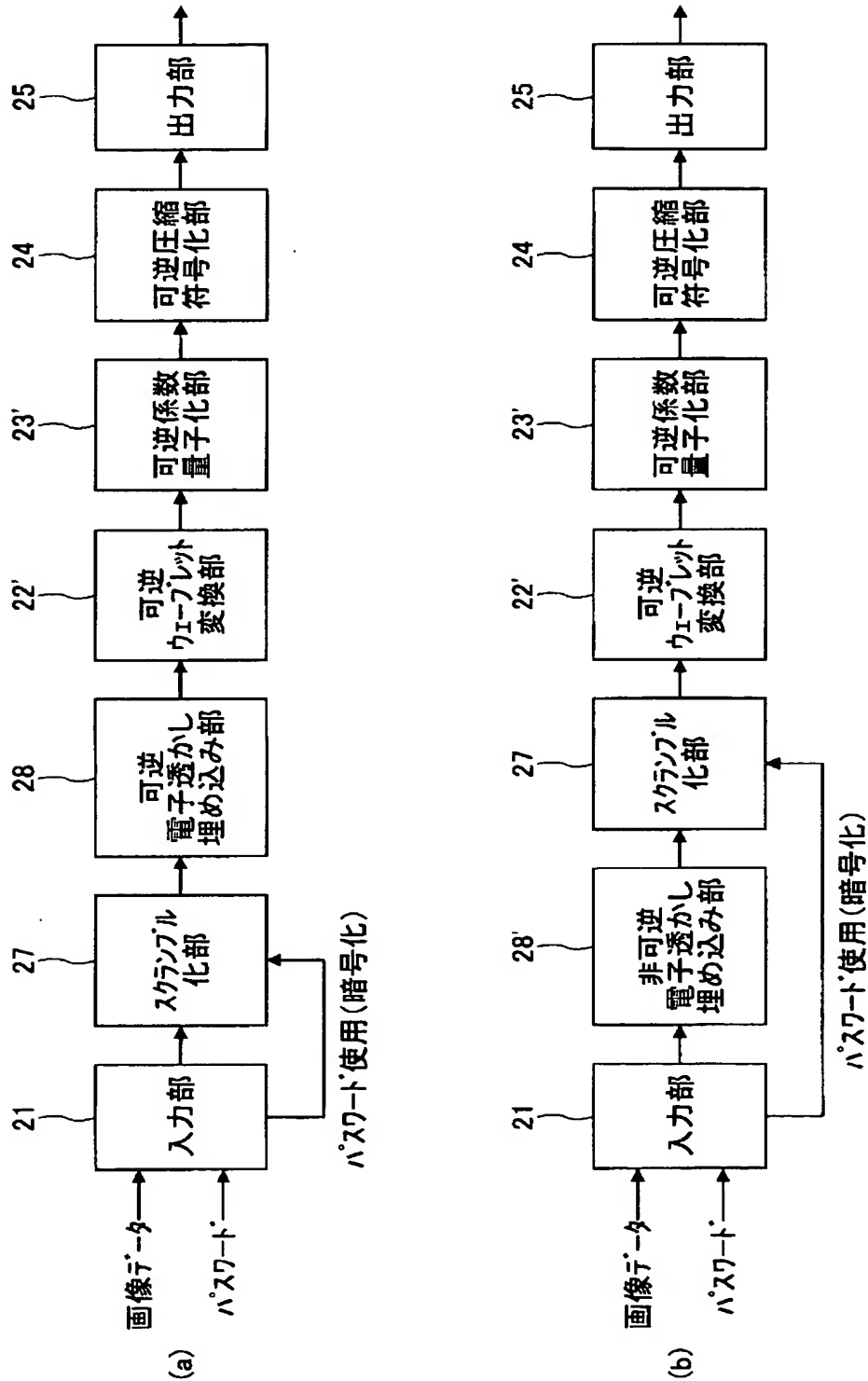
【図 12】

パーソナルコンピュータにおける符号復号化の
処理系を書き直して示す機能的ブロック図



【図 13】

サーバコンピュータにおける画像圧縮符号化の
処理系の変形例を示す機能的ブロック図



【書類名】 要約書

【要約】

【課題】 スクランブルの影響が残らない復号処理を可能にする。

【解決手段】 入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する圧縮符号化手段 2 6 に対して、この圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段 2 7 を設けることで、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後には可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数にスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、復号に際しては完全にスクランブルの影響をなくすることが可能となる。

【選択図】 図 9

特願 2 0 0 4 - 0 1 2 2 3 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー